

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-166999

(43)Date of publication of application : 22.06.2001

(51)Int.Cl.

G06F 12/14

G06F 12/16

(21)Application number : 11-348782 (71)Applicant : PIONEER ELECTRONIC
CORP

(22)Date of filing : 08.12.1999 (72)Inventor : NONAKA YOSHIYA
SHIBAZAKI HIROAKI

(54) METHOD AND DEVICE FOR RECORDING AND READING INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To realize recording for data backup while maintaining the concept of copy inhibition.

SOLUTION: At the time of backing-up original data recorded in a first recording medium 16, first enciphered information enciphered and recorded based on identification information (ID1) attached to the first storage medium is read, and the read first enciphered information is enciphered based on identification information (ID2) attached to a second recording medium 44 for backup so that second enciphered information can be generated, and the generated second enciphered information is recorded in a second recording medium. At the time of

restoring backup data, the second enciphered information is read from the second recording medium, and the second enciphered information is decoded based on the identification information of the second recording medium, and the decoded second enciphered information is restored as the first enciphered information, and recorded in the first recording medium.

LEGAL STATUS

[Date of request for examination] 08.06.2004

[Date of sending the examiner's
decision of rejection]

[Kind of final disposal of application
other than the examiner's decision of
rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] As opposed to the first record medium and second record medium with

which the identification information of a proper was given to each It is the information write reading approach of performing read of the information on which information was recorded or recorded. The first encryption information enciphered and recorded based on the identification information given to said first record medium is read. Encipher based on the identification information to which said first read encryption information was given by said second record medium, and the second encryption information is generated. Record said second generated encryption information on said second record medium, and the second encryption information is read in said second record medium. The information write reading approach characterized by what said second encryption information is decoded based on the identification information which said second record medium has, and said second decoded encryption information is restored as said first encryption information, and is recorded on said first record medium.

[Claim 2] The information write reading approach according to claim 1 characterized by permitting the read of each encryption information from the second record medium for a start [said] when authentication of the second record medium is performed and all are attested with the record medium of normal for a start [said].

[Claim 3] The first encryption information enciphered and recorded based on the identification information which the first record medium has is read. A reading means to be information write reading equipment which records the first encryption information concerned on the second record medium, and to read the first encryption information in said first record medium, An encryption means to encipher based on the identification information in which said second record medium has said first read encryption information, and to generate the second encryption information, Information write reading equipment characterized by having a record means to record said second generated encryption information on said second record medium.

[Claim 4] The aforementioned reading means is an information record reader according to claim 3 characterized by having further an authentication means to

perform authentication of the second record medium, and an authorization means to permit the read of said first encryption information when each of second record medium is attested with the record medium of normal for a start [said] by said authentication means, for a start [said].

[Claim 5] The second encryption information enciphered based on the identification information which the second record medium has is read. A reading means to be information write reading equipment which records the second encryption information concerned on the first record medium, and to read the second encryption information in said second record medium, Information write reading equipment characterized by having a decode means to decode said second encryption information based on the identification information which said second record medium has, and a record means to restore said second decoded encryption information as first encryption information, and to record on said first record medium.

[Claim 6] The aforementioned reading means is information write-reading equipment according to claim 5 characterized by having further an authentication means to perform authentication of the second record medium, and an authorization means to permit the read of said second encryption information when it is attested with each of second record medium being a record medium of normal for a start [said] by said authentication means, for a start [said].

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is used for the equipment which carries out record playback of the information, such as music, and an image or a computer program, and relates to the suitable information write reading approach and

equipment.

[0002]

[Description of the Prior Art] The distribution approach which distributes electronically information (work), such as music, and an image or a computer program, by communication link is becoming in use. The agreement which accepts only the distribution from the supply origin of informational normal is required of this distribution approach. That is, in the equipment which receives information, records this and is reproduced, the agreement which forbids the copy from one equipment to the equipment of another side must be carried out so that an illegal copy may overflow and great disadvantageous profit may not be produced to a copyright person. The condition that, as for a copy here, the same data exist on two or more kinds of media at coincidence is said.

[0003]

[Problem(s) to be Solved by the Invention] However, according to the above-mentioned agreement, it will not accept, even if it is a copy for backing up, and disadvantageous profit may be produced to the user who received the work to normal. For example, when the music stored in HDD (hard disk), an image, or program data is destroyed by a certain cause, it is necessary to receive again, and it cannot obtain depending on the case or, in the case of a program, it is also considered that it cannot respond with relation, such as version up.

[0004] In the information record reader which this invention is made in view of the above-mentioned situation, and has two or more record media When the information data recorded on the first record medium are recorded on the second record medium for backup, With the first record medium, it differs in those contents by enciphering and recording on the second record medium for backup based on the identification information of a proper. By this It aims at offering the information write reading approach and equipment which enable record for backing up, maintaining the concept of the ban on a copy.

[0005]

[Means for Solving the Problem] In order to solve the above-mentioned technical

problem the information write reading approach according to claim 1 It is the information write reading approach of performing read of the information by which information was recorded or recorded on each to the first record medium and second record medium to which the identification information of a proper was given. The first encryption information enciphered and recorded based on the identification information given to said first storage is read. Encipher based on the identification information to which said first read encryption information was given by said second record medium, and the second encryption information is generated. Record said second generated encryption information on said second record medium, and the second encryption information is read in said second record medium. We decided to decode said second encryption information based on the identification information which said second record medium has, to restore said second decoded encryption information as said first encryption information, and to record on said first record medium.

[0006] Moreover, in this approach according to claim 1, when authentication of the second record medium was performed and all were attested with the record medium of normal for a start [said], it was presupposed to the information write reading approach according to claim 2 that the read of each encryption information is permitted from the second record medium for a start [said].

[0007] In case the information recorded on the first record medium is recorded on the second record medium for backup, based on the identification information (the second identification information) of a proper, it is enciphered and recorded on the second record medium by this. The information recorded on the second record medium becomes what is different from the first encryption information since it is enciphered based on the second identification information, and stops that is, hitting the concept of the copy of reproducing the same information. Therefore, it becomes recordable [for backing up], maintaining the concept of the ban on a copy. Moreover, since it is carrying out performing mutual recognition in backup, generation of an unjust copy is not generated.

[0008] The first encryption information which information write reading equipment

according to claim 3 was enciphered based on the identification information which the first record medium has, and was recorded is read. A read means to be information write-reading equipment which records the first encryption information concerned on the second record medium, and to read the first encryption information in said first record medium, We decided to have an encryption means to encipher based on the identification information in which said second record medium has said first read encryption information, and to generate the second encryption information, and a record means to record said second generated encryption information on said second record medium.

[0009] Moreover, the information record reader according to claim 4 presupposed said reading means further that it has an authentication means to perform authentication of the second record medium, and an authorization means to permit the read of said first encryption information when each of second record medium is attested with the record medium of normal for a start [said] by said authentication means for a start [said] in this equipment according to claim 3.

[0010] An information record reader according to claim 5 reads the second encryption information enciphered based on the identification information which the second record medium has. A reading means to be information write-reading equipment which records the second encryption information concerned on the first record medium, and to read the second encryption information in said second record medium, We decided to have a decode means to decode said second encryption information based on the identification information which said second record medium has, and a record means to restore said second decoded encryption information as first encryption information, and to record on said first record medium.

[0011] Moreover, the information record reader according to claim 6 presupposed the aforementioned reading means further that it has an authentication means to perform authentication of the second record medium, and an authorization means to permit the read of said second encryption information when it is attested with each of second record medium being a record medium of normal

for a start [said] by said authentication means for a start [said] in this equipment according to claim 5.

[0012] When backing up the contents recorded on the first record medium to the second record medium, it is enciphered through an encryption means by the above-mentioned configuration. Encryption here extracts the identification information (ID) of a proper to the second record medium, and is performed by using as key data for enciphering this extracted identification information.

Therefore, the information enciphered by the identification information of the proper which the first record medium has will be enciphered here by the identification information which the second record medium has further. On the other hand, when the data (former data) recorded on the first record medium are destroyed by any cause, it is necessary to restore using the data (backup data) obtained from the second record medium. At this time, it restores to the data read from the second record medium, decode is performed based on the identification information which the second record medium has with a decode means, and that decoded information, i.e., the information enciphered by the identification information of the proper which the first record medium has, is written in the first record medium. It means that the information enciphered by only the identification information which the first record medium has by this was written in the first record medium.

[0013] The read for recording or restoring for backing up becomes possible, maintaining the concept of the ban on a copy by the above. In addition, since it is made when each of above-mentioned read and writing performs mutual recognition, an inaccurate copy or data do not disappear.

[0014]

[Embodiment of the Invention] Drawing 1 is drawing showing the operation gestalt of the information regeneration system as which this invention is adopted. The information regeneration system has the composition that playback information is enjoyed by the user in the home server 1 used as a sound source by carrying out powder arrangement of the wireless loudspeaker 3 which

becomes a nucleus with a man machine interface for two or more minutes. And the wireless loudspeaker 3 connected to a home server 1 is chosen with migration of the wireless terminal 2 which a user carries.

[0015] Drawing 2 is the block diagram showing the internal configuration of a home server 1 shown in drawing 1 . In drawing, 11 is CPU used as the control center of the home server 1 concerned used as a main phone. CPU11 decodes the command given by the user through the actuation key 12, and a processing result is displayed on a display 13, or it controls each block mentioned later. CPU11 is made by any above-mentioned control reading an internally stored program (not shown), and performing it serially. 14 is IDROM and is memory which mainly stores the unique identification number which the home server 1 concerned has.

[0016] 15 is a transceiver unit and a nucleus constitutes a control section 151 from the transmitting section 152 and a receive section 153. Under control by CPU11 and the control section 151, the transmitting section 152 becomes irregular through a multiplexer 17 and an encoder 18, and transmits the sound signal supplied by the address data bus 161 and 162 courses from the sound source of CD player 45, a tuner 46, and HDD16 grade to two or more wireless loudspeakers 3 used as a man machine interface. The signal supplied from the wireless terminal 2 or the wireless loudspeaker 3 is received under control by CPU11 and the control section 151, it restores by the decoder 19, and a receive section 153 downloads to HDD16 by the demultiplexer 20, the address data bus 161, and 162 courses if needed.

[0017] It shall be HDD for backup, and shall connect with the address data buses 161 and 162 as well as HDD16, music data shall be recorded and read under control by CPU11, and 44 shall be supplied to a reversion system as a sound source. The detail is shown in drawing 5 .

[0018] Drawing 3 is the block diagram showing the internal configuration of the wireless terminal 2 shown in drawing 1 . In drawing, 21 is CPU used as the control center of the wireless terminal 2 concerned used as a cordless handset.

CPU21 carries out read-out activation of the instruction code (the relay code mentioned later is included) showing the playback command stored in the instruction code storage section 25, a record command, etc., and also performs radial transfer by the actuation key 22 and the display 23. 24 is IDROM and the unique identification number (ID) of the wireless terminal concerned is mainly stored.

[0019] 26 is a transceiver unit and a nucleus constitutes a control section 261 from the transmitting section 262 and a receive section 263. The transmitting section 262 supplies the signal modulated through the encoder 42 to a home server 1 and the wireless loudspeaker 3 under control by CPU21 and the control section 261. A receive section 263 restores the received signal by the decoder 41 under control by CPU21 and the control section 261, and supplies CPU21 through a demultiplexer 43. The speech information recorded on HDD27 is changed into an analog signal through D/A converter 28 under control by CPU21, and is supplied to the pocket loudspeaker 30 which the wireless terminal 2 has by amplifier 29 course.

[0020] Drawing 4 is the block diagram showing the internal configuration of the wireless loudspeaker 3 shown in drawing 1. In drawing, 31 is CPU used as the control center of the wireless loudspeaker 3 concerned used as a cordless handset. CPU31 controls each block later mentioned according to the program to build in. 32 is IDROM and the unique identification number given to the wireless loudspeaker 3 concerned is the memory mainly stored.

[0021] 33 is a transceiver unit and a nucleus constitutes a control section 331 from the transmitting section 332, a receive section 333, and a field strength test section 334. The transmitting section 332 becomes irregular through an encoder 36, and supplies the signal generated by CPU31 to the wireless terminal 2 which is the home server 1 or cordless handset which is a main phone. A receive section 333 restores the sound signal received from the home server 1 which is a main phone by the decoder 37 under control by the control section 331, and supplies CPU31 by demultiplexer 38 course. The sound signal which CPU31

received is changed into an analog signal through D/A converter 39, by amplifier 34 course, is supplied to the loudspeaker 35 as a man machine interface, and is outputted as desired voice.

[0022] In addition, the field strength test section 334 is a part which measures the field strength of the relay code emitted from the wireless terminal 2 which is a cordless handset under control by CPU31, and the relay code sent with feeble power for the judgment of whether a user is in the about (for example, radius four way type of 50cm) three wireless loudspeaker concerned is used. The receiving result of a relay code is supplied to CPU31.

[0023] In the information regeneration system mentioned above, the information record reader of this invention is applied to a home server 1. HDD16 which is the former disk with which a home server 1 records the former data to which the identification information (ID) of a proper was given, respectively, It has HDD44 which is the disk for backup which records backup data. It is based on the medium ID (ID1) by which while it is a former disk was given to HDD16. For example, it is enciphered using the encoding technology good (Data Encryption Standard) and known. By enciphering based on the medium ID (ID2) to which the encryption information which read the recorded encryption information and was read here was given by HDD44 further for backup, the data for backup are generated and this generated encryption information is recorded on HDD44 for backup. On the other hand, when the former data currently recorded on HDD16 are destroyed by a certain reason, former data are restored from HDD44 for backup using the medium ID (ID2).

[0024] in addition -- if it is HDD by which ID which is the identification information of a proper is used for a record medium with this invention operation gestalt -- the fixed area (FAT:File Allocation Table) of a disk -- moreover, if it is an optical disk, it rewrites to a fixed area the same as a preformat, and is set up in the improper condition. By this invention, unless these record media are destroyed physically, it explains below at a detail on the assumption that ID is not rewritten.

[0025] Drawing 5 is the block diagram showing the detail of the circumference

circuit which HDD 16 and 44 of the home server 1 shown in drawing 1 has. The circumference circuit of HDD44 where the circumference circuit of HDD16 which serves as a former disk on A side serves as a backup disk on B side is shown among drawing.

[0026] The circumference circuit of HDD16 consists of the pickup unit 111, a demodulator 112, a modulator 113, decoders 114 and 118, ID extract circuit 115, drive CPU 116, a multiplexer 117, and a code machine 119. The circumference circuit of HDD44 consists of the pickup unit 120, a modulator 121, a demodulator 122, a code machine 123, drive CPU 124, and an ID extract circuit 125.

[0027] The pickup unit 111 in the circumference circuit of HDD16 is a read/write circuit containing the magnetic head prepared in order to perform read/write to the former disk 16. The contents written in here are generated by enciphering according to the medium ID in which the former disk 16 has input data supplied by communication link with the code vessel 119 from the exterior. Encryption here is made by supplying ID1 extracted by ID extract circuit 115 by drive CPU116 course. And pickup 111 is supplied by multiplexer 117 and modulator 113 course, and it writes in the former disk 16. Moreover, via a demodulator 112, encryption is solved with a decoder 114 and the data read from the former disk 16 are outputted to reversion systems (not shown), such as a D/A conversion circuit which a home server 1 has.

[0028] On the other hand, when backing up the contents recorded on the former disk 16 to HDD44, the contents read from the former disk 16 by pickup 111 and demodulator 112 course are enciphered with the code vessel 123 in the HDD44 circumference circuit shown in B side. The medium ID of HDD44 for backup extracted by ID extract circuit 125 (ID2) is supplied via drive CPU 124 under control of drive CPU 124, and encryption here is enciphered based on this ID. Therefore, the information enciphered by ID1 will be further enciphered by ID2 here.

[0029] When the data currently recorded on the former disk 16 are destroyed by any cause, the data obtained from a backup disk 44 are restored. It gets over

with a demodulator 122 and this data that came and was read from the backup disk 44 by the pickup 120 course is supplied to the decoder 118 of the circumference circuit of HDD16 under control of drive CPU 124. In a decoder 118, encryption by ID2 which is the medium ID of HDD44 for backup notified through drive CPU 116 is solved about the data obtained from a demodulator 122, ID2 is separated, and pickup 111 is supplied by multiplexer 117 and modulator 113 course. By this, the pickup unit 111 writes the information enciphered by only ID1 in the former disk 16.

[0030] In addition, although each of each blocks mentioned above was explained as hardware, the firmware in which drive 116 and CPUs 124 has a part may realize them.

[0031] Drawing 6 and drawing 7 are flow charts which show actuation of this invention operation gestalt, and the operations sequence of the drive CPU 124 in the case of backup record and the operations sequence of the drive CPU 116 in the case of restoration record are shown, respectively. As for (a), all show a subroutine, as for a main routine, (b), or (c).

[0032] Hereafter, actuation of this invention operation gestalt shown in drawing 5 is explained to a detail, referring to drawing 6 and drawing 7. First, drive CPU 124 performs mutual recognition processing between drives CPU 116 (step S61). As shown in drawing 6 (b), mutual recognition requires the authorization code beforehand defined to CPU116 (step S611), checks the authorization code (step S611), and if it is a predetermined code, when the authorization code of the drive CPU 124 defined beforehand is sent out to drive CPU 116 (step S613) and it is answered to ACK from drive CPU 116, it will be taken as an authentication success (step S614). When authentication ends in failure, it considers as an error (step S615).

[0033] Next, drive CPU 124 extracts the medium ID of a backup disk 44 (ID2) (step S62). And a data transfer demand is published to drive CPU 116 (step S63), it requires that former data should be supplied from the former disk 16, and record processing is performed based on the data (step S64). Based on ID2

supplied through drive CPU 124 with the code vessel 123, the former data (finishing [encryption by ID1]) obtained from a demodulator 112 are enciphered (step S641), a record modulation is carried out with a modulator 121, and record processing is made by what the contents are written in a backup disk 44 for by pickup 120 course (step S642), as shown in drawing 6 (c). And it confirms whether the data transfer of the desired specified quantity was completed (step S65), and in the case of no, the processing after step S63 is repeated, it waits for all transfer termination, and a backup process is finished.

[0034] Next, it explains, referring to the flow chart of drawing 7 about the restoration record processing by the backup disk 44 when former data are destroyed by a certain cause. First, drive CPU 116 performs mutual recognition processing (step S71). Mutual recognition processing is the same as that of the procedure shown by drawing 6 (b). Next, the Request to Send of ID2 which is the medium ID of a backup disk 44 is published to drive CPU 124 (step S72). And the data transfer from a backup disk 44 is required (step S73), and record processing to the former disk 16 is performed (step S74).

[0035] As record processing is shown in drawing 7 (b), drive CPU 116 decodes the backup data enciphered by the medium ID of HDD44 for backup obtained through a demodulator 122 (ID2) with a decoder 118 based on ID2 supplied at step S72 (step S741), and carries out a record modulation with a modulator 113 through a multiplexer 117 (step S742). The backup data by which the record modulation was carried out with the modulator 113 are written in the former disk 16 by pickup unit 111 course.

[0036] Next, it confirms whether the data transfer of the desired specified quantity was completed (step S75), and in the case of no, the processing after step S73 is repeated, it waits for all transfer termination, and restoration record processing is finished.

[0037] When this invention backs up above the former data recorded on the first record medium 16 like explanation, The first encryption information enciphered and recorded based on the identification information (ID1) given to the first

storage is read. The second encryption information which enciphered based on the identification information (ID2) to which the first read encryption information was given by the second record medium 44 for backup, generated the second encryption information, and was generated here is recorded on the second record medium. When restoring backup data, the second encryption information is read in the second record medium, it decodes based on the identification information in which the second record medium has the second encryption information, this second decoded encryption information is restored as first encryption information, and it records on the first record medium. A copyright person's right can be protected without attaining backup record by this and giving the user of normal disadvantageous profit.

[0038]

[Effect of the Invention] In the information write-reading equipment which has two or more record media like explanation above according to this invention By enciphering and recording them on the second record medium for backup based on the identification information of a proper, in case the information data recorded on the first record medium are recorded on the second record medium for backup The first record medium differs in those contents, and it enables record for backing up by this, maintaining the concept of the ban on a copy. Moreover, when the former data recorded on the first record medium by a certain cause are destroyed, the former reconstitution of data becomes possible at the first record medium by decoding based on the identification information which the second record medium has. Furthermore, since the above-mentioned record and restoration are performed by mutual recognition, an illegal copy can be prevented.

[0039] Therefore, while being able to aim at protection of the right to a copyright person, it becomes recordable [for backup], maintaining the concept of the ban on a copy further, so that disadvantageous profit may not arise to the user of normal, either, and becomes an effective means in future information and communication fields.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the example of the information playback structure of a system as which this invention is adopted.

[Drawing 2] It is the block diagram showing the internal configuration of the home server in drawing 1 .

[Drawing 3] It is the block diagram showing the internal configuration of the wireless terminal in drawing 1 .

[Drawing 4] It is the block diagram showing the internal configuration of the wireless loudspeaker in drawing 1 .

[Drawing 5] It is the block diagram having extracted and shown only the part related to this invention among the home servers shown in drawing 1 and drawing 2 .

[Drawing 6] It is drawing having shown the operations sequence of this invention operation gestalt with the flow chart.

[Drawing 7] It is drawing having shown the operations sequence of this invention operation gestalt with the flow chart.

[Description of Notations]

1 -- A home server, 2 -- A wireless terminal, 11 (21 31) -- CPU, 12 (22) -- An actuation key, 14 (24 32) -- IDROM, 15 (26 33) -- Transceiver unit, 16 (27) -- A hard disk drive unit (HDD), 44 -- Backup disk equipment (HDD), 112 [-- ID extract circuit, 116 (124) / -- Drive CPU, 117 / -- A multiplexer, 119 (123) / -- Code machine] (122) -- A demodulator, 113 (121) -- A modulator, 114 (118) -- A decoder, 115 (125)
